Audit Report

UNCLASSIFIED BUT SENSITIVE INTERNET PROTOCOL ROUTER NETWORK SECURITY POLICY

Report No. D-2001-017 December 12, 2000

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2885

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ANSOC	Army Network Security Operations Center
ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DISA	Defense Information Systems Agency
DISA-RNOSC-C	Defense Information Systems Agency, Regional Network Operations and Security Center, Columbus
DISN	Defense Information System Network
FORSCOM	U.S. Army Forces Command
GIG	Global Information Grid
ISP	Internet Service Provider
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
ODISC^4	Office of the Director of Information Systems for Command, Control, Communications, and Computers

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

December 12, 2000

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on the Unclassified but Sensitive Internet Protocol Router Network Security Policy (Report No. D-2001-017)

We are providing this audit report for information and use. This is one of a series of reports regarding DoD efforts to increase the security posture of the Unclassified but Sensitive Internet Protocol Router Network. We considered management comments on a draft of this report when preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Ms. Wanda A. Hopkins at (703) 604-9049 (DSN 664-9049) (wahopkins@dodig.osd.mil), or Ms. Dianna J. Pearson at (703) 604-9063 (DSN 664-9063) (djpearson@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-017 **December 12, 2000**
(Project No. D2000AS-0085)

Unclassified but Sensitive Internet Protocol Router Network Security Policy

Executive Summary

Introduction. The Unclassified but Sensitive Internet Protocol Router Network is a network of government-owned Internet protocol routers used to exchange unclassified but sensitive information between DoD users. The Unclassified but Sensitive Internet Protocol Router Network is also the primary entrance into the Internet. As of August 2000, over 70 percent of Unclassified but Sensitive Internet Protocol Router Network traffic is directed toward the Internet. As the growth and usage of the Internet surge, so do the dangers of intrusion into sensitive networks. In a policy memorandum on "Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network," August 22, 1999, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) expressed interest and concern over the multitude of interconnections between the Unclassified but Sensitive Internet Protocol Router Network and the Internet.

Objective. The overall audit objective was to evaluate DoD efforts to increase the security posture of the Unclassified but Sensitive Internet Protocol Router Network.

Results. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) did not have an active Unclassified but Sensitive Internet Protocol Router Network security policy and lacked visibility of unauthorized Internet access connections because the August 1999 policy memorandum and accompanying implementation guidelines expired in November 1999 and did not:

- clearly define the direct Internet connection waiver process, including the roles, responsibilities, and timelines for reviewing, validating, and approving waiver requests; and

- provide implementing details for DoD Components to report monthly on progress and issues relating to the Unclassified but Sensitive Internet Protocol Router Network transition process.

The memorandum was never formally incorporated into Defense policy. As a result, the requirement for DoD Components to follow the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Unclassified but Sensitive Internet Protocol Router Network security policy memorandum and implementation guidelines has been unenforceable since November 1999. Although the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) initiated efforts to increase the security posture of the Unclassified but Sensitive Internet Protocol Router Network by initiating preliminary policy and guidance, additional efforts were needed to incorporate that policy and guidance into a DoD directive or regulation. The lack of current policy guidelines was a material management control weakness (finding A).

In the absence of DoD guidance, individual installations and commands may have made questionable decisions on commercial Internet access. For example, Fort Irwin, California, had a questionably necessary direct commercial Internet connection without proper authorization. As a result, the ability of Defense Information Systems Agency to maintain comprehensive control of the Unclassified but Sensitive Internet Protocol Router Network is impaired and the security posture of the Unclassified but Sensitive Internet Protocol Router Network put at greater risk (finding B).

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) immediately establish enforceable interim guidance that clearly defines requirements to increase the security posture of the Unclassified but Sensitive Internet Protocol Router Network; expedite the issuance of a DoD directive, instruction, or regulation; and establish a tracking system for all approved waiver requests to enable timely periodic reevaluations of those waivers.

We recommend that the Commander, Fort Irwin, coordinate with the Defense Information Systems Agency to identify and implement needed technical solutions to Fort Irwin's problems connecting to the Internet via the Unclassified but Sensitive Internet Protocol Router Network. We also recommend that the Commander, Fort Irwin, disconnect the commercial Internet connection until an Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) waiver is obtained or a technical solution is developed.

Management Comments. The Director, Architectures and Interoperability Directorate, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (Deputy Chief Information Officer), provided an overview of the Global Information Grid Waiver Board and Waiver Panel. The Global Information Grid Network Waiver Review Panel's initiative is to publish clear criteria to be used in the adjudication of Unclassified but Sensitive Internet Protocol Router Network waiver requests. The Director stated that he sees a requirement for a DoD Directive and a DoD Instruction. The milestone for this issuance is February 2001. The Director stated that he has closely collaborated with the Defense Information Systems Agency waiver staff and requires a stringent tracking mechanism for all waivers.

Fort Irwin concurred with all the recommendations. Fort Irwin coordinated through U.S. Army Forces Command, who in turn coordinated with the Defense Information Systems Agency, and has restructured the path and increased the bandwidth by which Fort Irwin reaches the Internet via the Unclassified but Sensitive Internet Protocol Router Network. Furthermore, Fort Irwin disconnected the commercial Internet connection and requested that the waiver request be withdrawn. Although not required to comment, the U.S. Army Forces Command concurred with the recommendations, but disagreed with some information in the report. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Audit Response. Although the Director, Architectures and Interoperability Directorate, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (Deputy Chief Information Officer), did not specifically state concurrence or nonconcurrence with the recommendations, the management comments are responsive. The Fort Irwin comments were responsive.

Table of Contents

Background

Joint Vision 2010 and 2020. In planning, directing, coordinating, and executing missions, DoD relies on critical digital electronic information capabilities to store, process, and move essential data. In 1996, the Chairman of the Joint Chiefs of Staff issued a conceptual template, "Joint Vision 2010," that stressed the need for information superiority, which is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. The effort to achieve and maintain information superiority invites attacks on DoD information systems. To build on and extend the conceptual template established by Joint Vision 2010, the Chairman of the Joint Chiefs of Staff issued "Joint Vision 2020," in 2000. Joint Vision 2020 stresses the importance of full-spectrum dominance—the ability of U.S. forces to defeat any adversary and to control any situation across the full-range of military operations. Information superiority and information assurance are key components of full-spectrum dominance.

Information Assurance. Information assurance is emerging as a critical component of DoD operational readiness. Information assurance consists of actions that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. It includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Effective information assurance enables information systems and networks within the Defense information infrastructure to provide protected, continuous, and dependable service in support of both warfighting and business missions.

Defense Information System Network. The Defense Information System Network (DISN) is the DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. The Defense Information Systems Agency (DISA) has overall program responsibility for DISN. DISN provides a full range of communication services—voice, data, and video to the warfighter and support elements. DISN encompasses the following telecommunications subsystems and networks: the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet), the Secret Internet Protocol Router Network (SIPRNet), and the Integrated Digital Network Exchange. DISN is an important element of the DoD Global Information Grid (GIG)[1].

In May 1996, the Chairman of the Joint Chiefs of Staff established DISN as the primary DoD end-to-end telecommunications network for supporting military operations. All DoD activities requiring Internet and telecommunications services were directed to use DISN when those services were available and technically and economically feasible. In December 1998, the Deputy Secretary of Defense reinforced the policy by revising Program Budget Decision 417C, "Information Services," that directed DoD Components to obtain

[1]The DoD Global Information Grid is a globally interconnected end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

communications services for existing or planned systems through DISA and DISN beginning in FY 2000. Exclusion from DISN use required a specific waiver, based on mission need, from a board, referred to as the GIG Waiver Board, established by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C^3I)]. The Under Secretary of Defense (Comptroller), Director, Program Analysis and Evaluation, and Under Secretary of Defense (Acquisition, Technology, and Logistics) also participate as voting members of the board.

On August 24, 2000, the Deputy Secretary of Defense issued a policy memorandum, "Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 4-8460 - Department of Defense Global Information Grid Networks," that updated the GIG policy which provides direction and assigns responsibilities for effective, efficient, and economical acquisition, management, and use of network equipment and services. Specifically, the August 2000 GIG policy instructions reinforced the requirement that the DISN shall be the means for DoD-wide networking, unless granted a waiver through the GIG Waiver Board process.

NIPRNet. NIPRNet is a network of government-owned internet protocol routers used to exchange unclassified but sensitive information between DoD users. NIPRNet was created as a replacement for the Defense Data Network in 1995 and is the primary entrance into the Internet from the DISN. As of August 2000, over 70 percent of NIPRNet traffic is directed toward the Internet. Since its inception, the NIPRNet has grown substantially every year and is predicted to continue to grow. There are approximately 1,500 full-time user connections to the NIPRNet and potentially over one million users total. Deployed forces can also access the NIPRNet through the use of the Integrated Tactical-Strategic Data Network. See Appendix C for information on the number of customer connections and the bandwidth requirements for the NIPRNet, and information on the NIPRNet redesign effort. As the number of NIPRNet to Internet connections increase, the more difficult it is to manage and control access to DoD systems connected to the NIPRNet.

NIPRNet Security Policy. In a policy memorandum "Increasing the Security Posture of the NIPRNet," August 22, 1999, the ASD(C^3I) expressed interest and concern over the multitude of interconnections between the NIPRNet and the Internet. Positive control of military connections to the Internet is an absolute requirement to support the setting of the information operations condition[2]. The ASD(C^3I) stated that uncontrolled Internet connections pose a significant threat to all DoD information systems and operations. See Finding A for more information on the NIPRNet security policy.

[2]Chairman of the Joint Chiefs of Staff memorandum CM-510-99, "Information Operations Condition," March 10, 1999, defines information operations condition as a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent.

Objective

The overall audit objective was to evaluate DoD efforts to increase the security posture of the NIPRNet. See Appendix A for a discussion of the audit scope and methodology. See Appendix B for prior coverage related to the audit objective.

A. Adequacy of NIPRNet Security Policy and Implementation Guidelines

The ASD(C³I) did not have an active NIPRNet security policy and lacked visibility of unauthorized Internet access connections because the ASD(C³I) established a policy memorandum and accompanying implementation guidelines that:

- expired in November 1999;
- did not clearly define the direct Internet connection waiver process, including the roles, responsibilities, and timelines for reviewing, validating, and approving waiver requests;
- did not provide implementing details for DoD Components to report monthly on progress and issues relating to the NIPRNet transition process; and
- were never formally incorporated into Defense policy.

As a result since November 1999, the requirement for DoD Components to follow the ASD(C³I) NIPRNet security policy memorandum and implementation guidelines was unenforceable and DoD lacked effective management controls for Internet access.

NIPRNet Security Policy Memorandums and Implementation Guidelines

To increase the security posture of the NIPRNet, the ASD(C³I) issued a policy memorandum, "Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet)," August 22, 1999, that mandated the use of the NIPRNet as the only DoD authorized access to the Internet. Specifically, the policy memorandum stated that by December 15, 1999, all DoD components should only use authorized NIPRNet-Internet connections. Additionally, the ASD(C³I) issued NIPRNet implementation guidelines that defined an authorized NIPRNet-Internet connection as an automated information system or network that:

- connected to the Internet through a NIPRNet-gateway, or
- connected to the Internet through an ASD(C³I) approved DoD Component Internet gateway (direct connection to the Internet).

The goal of the policy memorandum was to have DoD Components terminate all direct connections to the Internet and establish connectivity to the Internet via the NIPRNet by December 15, 1999. ASD(C³I) recognized that some DoD Components may require a direct connection to the Internet or that a near-term migration to the NIPRNet by all DoD Components may not be feasible.

Therefore, the ASD(C³I) established a waiver process to review each exception request and allow for a phased migration of systems to the NIPRNet. Internet connections that could not be terminated prior to December 15, 1999, needed an ASD(C³I) approved waiver.

Waiver Request Process

The ASD(C³I) NIPRNet policy memorandum stated that detailed information on waiver requests would be published in the accompanying implementation guidelines. However, the implementation guidelines did not provide detailed information about the waiver process, such as the DoD Component roles and responsibilities, or the timelines for reviewing, validating, and approving the waiver requests. Additionally, the policy memorandum did not address the issue of establishing expiration dates for any waivers, which would require periodic reassessment of approved waivers. Without an established timeframe for waiver reassessment, ASD(C³I) lacks the ability to monitor and manage approved waivers. Further, without a specific waiver time limit, DoD Components may erroneously believe that the approved waivers are permanent. The implementation guidelines stated that DoD Components should submit waiver requests to the DISN Security Accreditation Working Group, through the DISA NIPRNet website, by October 15, 1999, and stated that the DISN Security Accreditation Working Group should review and recommend to the ASD(C³I) the approval or disapproval of submitted waivers. However, the DISA NIPRNet website provides only a general overview of the waiver process that directs users through the waiver request template.

In January 2000, the ASD(C³I) developed the GIG Network Provisioning Process to establish a waiver process to handle all requests, including NIPRNet waiver requests. Although the ASD(C³I) has taken steps to establish the process, the information is fragmented. As of August 2000, the ASD(C³I) had not incorporated the GIG Network Provisioning Process into the existing waiver process. However, on August 24, 2000, the Deputy Secretary of Defense directed the Chief Information Officer, DoD, whose office resides with ASD(C³I), to incorporate the GIG network guidance into the DoD Directive System by February 2001.

Details for Standardized Reporting Requirements

The policy memorandum stated that DoD Components and DISA are required to brief the ASD(C³I) on NIPRNet transition progress and issues monthly, beginning in August 1999. The policy memorandum stated that detailed formats for monthly reporting were published in the implementation guidelines. However, according to the implementation guidelines, every Service and Agency would start monthly reporting to the ASD(C³I) effective September 30, 1999. Despite the requirements for monthly reports, as of August 2000, ASD(C³I) had not determined the report format. Specifically, there were no detailed instructions on who should submit reports (those with or those without NIPRNet connections, or both), when reports were due, who the reports should

be submitted to (either the ASD(C³I) or DISA), or the type of information to be reported. Also, there was no indication if DoD components would receive feedback on the reports submitted.

Status of Implementation Guidelines

The August 1999 policy memorandum and implementation guidelines stated that as of December 15, 1999, all DoD components were required to use only authorized NIPRNet-Internet connections. However, ASD(C³I) continued to label the implementation guidelines as "final draft" until February 16, 2000. Consequently, DoD Components were hesitant to implement the requirements in the guidelines because there was no formal acknowledgement from ASD(C³I) that the implementation guidelines were official policy and effective immediately. Additionally, the ASD(C³I) dated the guidelines January 6, 2000, even though removal of the "final draft" designation did not occur until February 2000. Although the implementation guidelines were available to DoD Components on the DISA NIPRNet-website, DoD Components may not have been aware of the change since there was no formal distribution or notification by ASD(C³I).

DoD Directives System

DoD Directive 5025.1, "DoD Directives System," June 24, 1994, states that policy memorandums must be reissued as DoD directives, instructions, or publications within 90 days of original issue date. Because the ASD(C³I) has not incorporated the August 1999 policy memorandum and implementation guidelines into a DoD directive, instruction, or regulation, the guidance on NIPRNet security and waiver requirements is not mandatory. As of August 2000, the ASD(C³I) has not issued any mandatory policy concerning NIPRNet-Internet requirements, but has been tasked by the Deputy Secretary of Defense to incorporate GIG network policies into DoD issuance by February 2001.

Summary

The protection of the NIPRNet is fundamental to the security of the DoD information infrastructure. Uncontrolled Internet connections pose a significant threat to all DoD information systems and operations, and therefore positive control of all connections to the Internet is an absolute requirement. Although the ASD(C³I), in conjunction with DISA, initiated efforts to increase the security posture of the NIPRNet by initiating preliminary policy and guidance, additional efforts are needed to incorporate that policy and guidance into a DoD directive or regulation. Unless the ASD(C³I) establishes clearly defined NIPRNet policy and implementation requirements, DoD efforts to increase the security posture of the NIPRNet will be hampered. The absence of meaningful guidelines is a material management control weakness.

Recommendations, Management Comments, and Audit Response

A. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

1. Immediately establish enforceable interim guidance that clearly defines requirements to increase the security posture of the Unclassified but Sensitive Internet Protocol Router Network, such as:

(a) the direct Internet connection waiver process including the establishment of definitive roles, responsibilities, and timelines for reviewing and approving waiver requests.

(b) the details for DoD components to report monthly on progress and issues relating to the Unclassified but Sensitive Internet Protocol Router Network transition process.

Management Comments. The Director, Architectures and Interoperability Directorate, Office of the ASD(C^3I), Deputy ASD(C^3I) (Deputy Chief Information Officer) [the Director], provided an overview of the GIG Waiver Board. Specifically, the Director stated that the ASD(C^3I) in his role as the DoD Chief Information Officer chairs the Waiver Board, and to add depth to the process, the Waiver Board had added the following three Board members: Joint Staff/J6; Director, DISA; and the Chief Information Officer of the DoD component requesting the waiver.

In March 2000, the Waiver Board established a GIG Network Waiver Review Panel to administer the process. The GIG Network Waiver Review Panel had eliminated a backlog of 121 NIPRNet waiver issues. Since then, waivers had been generally adjudicated within two weeks of DISN Security Accreditation Working Group review. If the waiver was granted, the duration of the waiver was only as long as deemed necessary, or for one year, whichever was sooner. The GIG Network Waiver Review Panel's initiative is to publish clear criteria to be used in the adjudication of NIPRNet waiver requests.

The Chairman of the GIG Network Waiver Review Panel routinely briefs each regular session of the Chief Information Officer Executive Board on the progress of the NIPRNet certification effort, and as a result, the DoD component Chief Information Officers have sharpened their focus on attaining certification and on providing timely progress reports. Additionally, the comments to Recommendation A.2., stated that the milestone for the issuance of a DoD Directive and a DoD Instruction is February 2001.

Audit Response. Although the Director did not specifically state concurrence or nonconcurrence with the recommendations, the management comments are responsive.

2. Expedite the issuance of a DoD directive, instruction, or regulation that will incorporate the interim guidance in Recommendation A.1.

Management Comments. The Director stated he sees a requirement for both a DoD Directive and a DoD Instruction. The directive will incorporate the intent of the ASD(C^3I) policy memorandum, "Increasing the Security Posture of the NIPRNet," August 22, 1999, as well as the major precepts expressed in DoD Chief Information Officer Guidance and Policy Memorandum No. 4-8460, "DoD Global Information Grid Networks," August 24, 2000, and Memorandum No. 10-8460, "Network Operations," August 24, 2000. The ASD(C^3I) tasked the Chairman of the GIG Network Waiver Review Panel to document the waiver process in a DoD Instruction. The instruction will also incorporate the interim guidance outlined in Recommendation A.1. The milestone for the issuance is February 2001.

Audit Response. Although the Director did not specifically state concurrence or nonconcurrence with the recommendations, the management comments are responsive.

3. Establish a tracking system for all approved waiver requests to enable timely periodic reevaluations of those waivers.

Management Comments. In comments to Recommendation A.1., the Director stated that the DISA NIPRNet staff tracks waived solutions. In comments to Recommendation A.3., the Director stated that the Chairman of the GIG Network Waiver Review Panel has closely collaborated with the DISA waiver staff to define the requisite elements of the waiver database, and to emphasize the DoD CIO oversight of the waiver tracking process. The Director stated that the GIG Network Waiver Process website will soon be expanded to incorporate the NIPRNet connection approval process policies and procedures.

Audit Response. Although the Director did not specifically state concurrence or nonconcurrence with the recommendations, the management comments are responsive.

B. Status of Fort Irwin's Direct Internet Connection Waiver Request

Fort Irwin, California, had a questionably necessary direct commercial Internet connection without appropriate authorization. This occurred because:

- Fort Irwin obtained a direct commercial Internet connection before determining whether the Army Network and Systems Operation Center (ANSOC) or the DISA, Regional Network Operations and Security Center, Columbus (DISA-RNOSC-C), could resolve connection problems to the Internet via the NIPRNet; and

- U.S. Army Forces Command (FORSCOM) and Army Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC[4]) delayed the processing of the Fort Irwin waiver request for the direct commercial Internet connection.

As a result, the ability of DISA to maintain comprehensive control of the NIPRNet is impaired and the security posture of the NIPRNet put at greater risk.

Fort Irwin Information Management

Fort Irwin is home to the National Training Center, which is the Army's premier training facility for mechanized and armor brigades. FORSCOM is the Major Command for Fort Irwin. The Fort Irwin Wide-Area Network provides digital communications to support electronic mail, resource sharing, Internet access, and a state-of-the-art communication infrastructure necessary for the various telecommunications needs. The Directorate of Information Management provides overall management and oversight for all functions pertaining to the engineering, monitoring, and support of the Fort Irwin network and all subordinate networks. The Directorate of Information Management's overall focus for networking was to ensure that efficient, cost-effective, and timely data communication technologies were made available to the warfighter and supporting elements.

Fort Irwin's Connections to the Internet

Fort Irwin uses two different methods to connect to the Internet. One method allows connection to the Internet via the NIPRNet and the other method provides a direct Internet connection through a commercial Internet service provider (ISP). Both connections to the Internet go through an intrusion detection system and Army security router (see Figure 1).

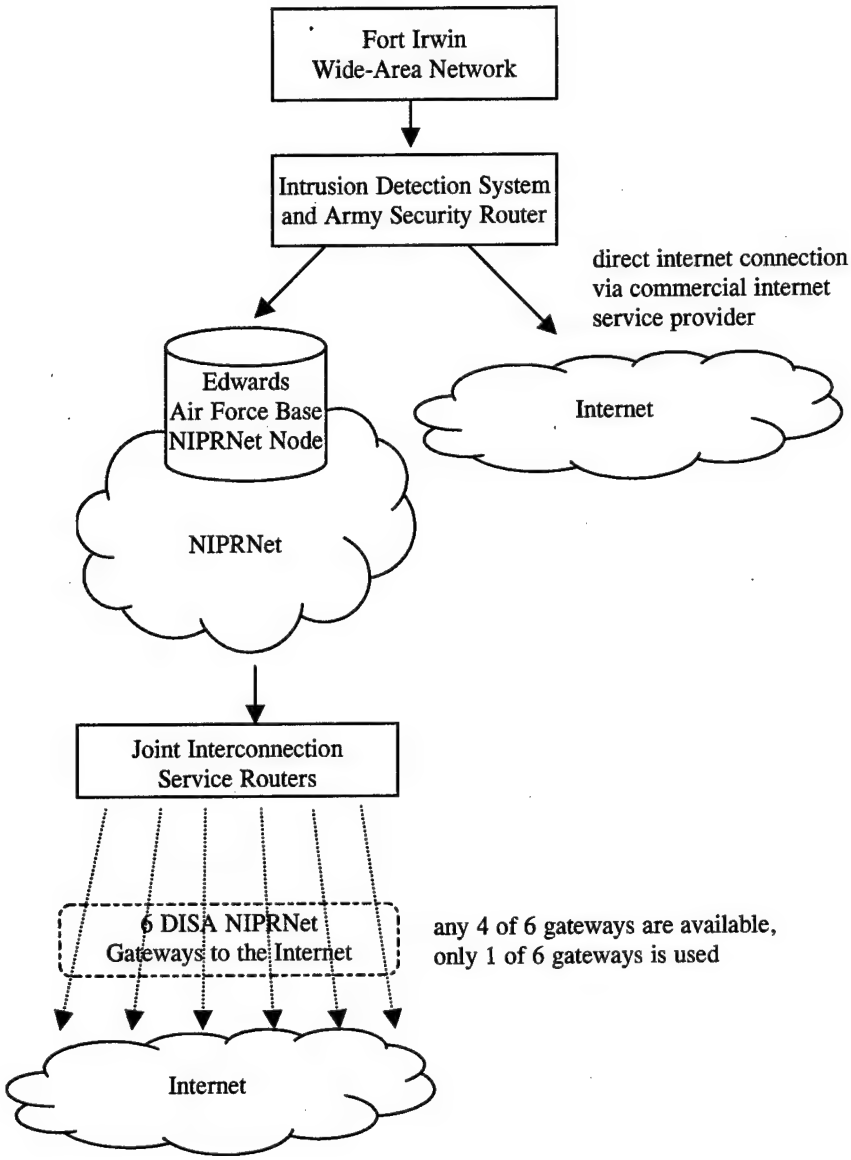


Figure 1. Fort Irwin's Connections to the Internet

For Fort Irwin to access the Internet via the NIPRNet, Fort Irwin must connect to a NIPRNet node located at Edwards Air Force Base, California. From Edwards Air Force Base, the traffic moves to the NIPRNet backbone, which is the core router directly connected to the Joint Interconnection Service routers. The Joint Interconnection Service routers provide entry points to the Internet through six NIPRNet authorized gateways. DISA configured the NIPRNet-Internet routing structure so that at any given time, any four of the six authorized gateways were always available.

Fort Irwin's Problems Connecting to the Internet via NIPRNet

In mid 1999, Fort Irwin personnel from the Directorate of Contracting reportedly experienced problems connecting to the Internet via the NIPRNet and were not able to meet work requirements. Without authorization from the Fort Irwin Director of Information Management, the contracting personnel installed personal ISP software on Government computers and used that software to connect to the Internet. Consequently, the Fort Irwin Designated Approving Authority disapproved the accreditation[3] of those government computers loaded with unauthorized personal ISP software. However, the Deputy Director of Contracting asked permission from the Fort Irwin Chief of Staff to leave the unauthorized software on the government computers. Although the Fort Irwin Chief of Staff approved the use of unauthorized ISP software, the Fort Irwin Director of Information Management did not agree because the setup did not comply with DoD and Army policy and security protection measures.

Reporting Network Related Problems. Fort Irwin reported all network-related problems, including NIPRNet problems, to ANSOC. ANSOC, which is part of the Army Signal Command, consists of teams that provide system, network, and database management support on a worldwide basis. ANSOC also had a help desk that provided 24-hour network monitoring services within several specified regions. ANSOC monitored Internet traffic for security purposes and bandwidth use. If Fort Irwin had a problem, ANSOC would first try to resolve it, but if unable to do so, would report to DISA-RNOSC-C. DISA-RNOSC-C was a central point of contact for documenting, disseminating, and orchestrating resolution of information technology problems. One of the primary responsibilities of DISA-RNOSC-C was support of the NIPRNet and its participants.

Fort Irwin Information Management personnel stated that they submitted numerous trouble calls to ANSOC about Internet connections via the NIPRNet, but received no satisfactory response. However, we were not able to document any record of trouble calls made to ANSOC or DISA-RNOSC-C by Fort Irwin since mid 1999.

Approval for Direct Connection to the Internet. In July 1999, Fort Irwin requested and FORSCOM approved a direct Internet connection through a commercial ISP without first determining whether ANSOC or DISA could resolve or had resolved NIPRNet-Internet connection problems. The FORSCOM approval of the Fort Irwin direct Internet connection through a commercial ISP included several restrictions:

[3]Part of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) which provides for the formal declaration by a designated approving authority that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

- the commercial ISP service would be user funded,
- the commercial ISP service would be connected to the Army security router at Fort Irwin, and
- Fort Irwin would have to submit a waiver request to the ASD(C³I) when the NIPRNet policy was issued.

The FORSCOM approval stated that if the waiver request was not approved, the direct Internet connection would be terminated. On receiving approval from FORSCOM, Fort Irwin issued a contract for a direct Internet connection on August 1999, with a period of performance ending on September 30, 2000. In September 1999, Fort Irwin requested the Army Signal Command to provide engineering support in connecting the commercial ISP to the Fort Irwin network. At that time, the Army Signal Command inquired about the FORSCOM position in granting approval for the direct Internet connection considering that the ASD(C³I) had just issued its NIPRNet policy and implementation guidelines. However, Army ODISC⁴ and FORSCOM approved the commercial ISP connection and reemphasized earlier restrictions and added that at the end of the commercial contract, Fort Irwin should only connect to the Internet via NIPRNet.

In October 1999, ANSOC installed and activated the commercial ISP to the Fort Irwin network, which was still in use in August 2000.

Waiver Request Status. Fort Irwin submitted a waiver request for its direct Internet connection in October 1999. As of August 2000, the Fort Irwin waiver request was awaiting FORSCOM validation. Subsequent to FORSCOM validation, Army ODISC⁴ validation was required before the waiver request was processed at the next approval level. As of August 2000, FORSCOM and Army ODISC⁴ had not processed the Fort Irwin waiver request for the direct commercial Internet connection.

The NIPRNet-Internet waiver request process guide, as described on the DISA NIPRNet website, requires the major command (second echelon) and the service headquarters element to validate the waiver request so that the request may proceed to the next level. Additionally, as part of the Army Network Security Improvement Program Guidance, the Army issued "Guidance for Complying with the August 22, 1999, ASD(C³I) Memorandum on NIPRNet-Internet Connectivity," September 20, 1999, which provided Army major commands, program executive offices, program managers, and other materiel developers and activities guidance for complying with the ASD(C³I) August 1999 policy memorandum. This guidance applied to the active Army, the Army National Guard, and the Army Reserve and was effective immediately. The Army guidance stated that major commands' information assurance officers were responsible for ensuring that all direct Internet connection waiver data was reported, and responsible for validating the accuracy of data provided by subordinate activities.

The ASD(C³I) policy memorandum required an approved waiver request for any Internet connections that did not operate through the NIPRNet. The ex post facto Fort Irwin waiver request remained unresolved and could not be

considered for further review until FORSCOM and Army ODISC[4] reviewed and validated the waiver request. Meanwhile, Fort Irwin operated an unauthorized NIPRNet-Internet connection.

Summary

Fort Irwin personnel reportedly experienced problems connecting to the Internet via NIPRNet and installed commercial ISP software on government computers to accomplish work requirements. The fact that Fort Irwin personnel installed and used personal ISP connections, with or without approval, increased the risk to the security posture of the Fort Irwin network and the NIPRNet. Although Fort Irwin subsequently received approval from FORSCOM and Army ODISC[4] for the direct commercial Internet connection, FORSCOM and Army ODISC[4] delayed in processing the waiver request and therefore the connection operated without an approved waiver. Fort Irwin's problems connecting to the Internet via NIPRNet might have been resolved if the activity had properly coordinated with ANSOC and DISA to determine the cause and find the solution to the connection problems. Until FORSCOM and Army ODISC[4] complete their review and validate Fort Irwin's waiver request, Fort Irwin will continue to operate with an unauthorized NIPRNet-Internet connection.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Commander, Fort Irwin:

1. Coordinate with the Defense Information Systems Agency to identify and implement needed technical solutions to Fort Irwin's problems connecting to the Internet via the Unclassified but Sensitive Internet Protocol Router Network.

2. Disconnect the commercial Internet connection until an Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) waiver is obtained or a technical solution is developed.

Fort Irwin Comments. Fort Irwin concurred with both recommendations. Fort Irwin stated that they have coordinated with FORSCOM, which in turn coordinated with DISA, and has restructured the path and increased the bandwidth by which Fort Irwin connects to the Internet via the NIPRNet. Also, Fort Irwin stated that the Fort Irwin commercial Internet connection was disconnected on September 29, 2000. In addition, as of October 10, 2000, Fort Irwin has requested through FORSCOM to withdraw the waiver request.

U.S. Army Forces Command Comments. Although not required to comment, FORSCOM concurred with the recommendations. However, FORSCOM disagreed that FORSCOM delayed in the processing of the waiver request. FORSCOM stated that there was no clear guidance from DoD that defined the roles in the internet waiver process. Also, FORSCOM stated that they were actively involved in the waiver process and took numerous actions to work with

Fort Irwin and DISA. FORSCOM also disagreed that due to the Fort Irwin direct Internet connection, the ability of DISA to maintain control of the NIPRNet was impaired and the security posture of the NIPRNet put at greater risk. FORSCOM stated that the Fort Irwin direct Internet connection went through the Army security router, just like the NIPRNet traffic. FORSCOM believes that risks at Fort Irwin are minimal.

Audit Response. As stated in Finding A, we recognize that the ASD(C^3I) did not clearly define the direct Internet connection waiver process. However, from October 1999 to August 2000, the Fort Irwin waiver request was awaiting FORSCOM validation. Additionally, in order to maintain proper NIPRNet network management and security, DISA needs to know all of the direct connections between the NIPRNet and Internet.

Appendix A. Audit Process

Scope

Work Performed. We reviewed and evaluated NIPRNet security guidance contained in the ASD(C^3I) memorandums, "Increasing the Security Posture of the NIPRNet," August 22, 1999, and "Extending Deadlines Relating to the Memorandum, 'Increasing the Security Posture of the NIPRNet,'" September 7, 1999, and the accompanying implementation guidelines. We reviewed the NIPRNet connection approval process website, established by DISA, for use by DoD Components to register NIPRNet connections and to apply for waivers of direct Internet or user enclave connections.

We visited Fort Irwin, California, to evaluate its NIPRNet connection and direct Internet connection. We also visited the Army Signal Command, Fort Huachuca, Arizona, to gain an understanding of the ANSOC process for resolving NIPRNet trouble calls, specifically for Fort Irwin. Additionally, we visited the DISA-RNOSC-C in Columbus, Ohio, to gain an understanding of the DISA-RNOSC-C role in the NIPRNet, and to see how it resolves NIPRNet trouble calls. The Technical Assessment Division for the Office of the Inspector General, DoD, assisted in reviewing and evaluating the NIPRNet security policy memorandum and accompanying implementation guidelines, as well as the NIPRNet connection and direct Internet connection at Fort Irwin.

DoD-Wide Corporate Level Government Performance and Results Act Goals (GPRA). In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. Although the Secretary of Defense has not established any DoD goals for Information Assurance, the General Accounting Office lists it as a high-risk area. This report pertains to Information Assurance as well as to achievement of the following goals.

DoD-Functional Area Reform Goals. Most DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals:

- **Information Technology Management Functional Area.** **Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate Defense information infrastructure. **(ITM-2.2)**

- **Information Technology Management Functional Area.** **Objective:** Ensure DoD vital information resources are secure and protected. **Goal:** Build information assurance framework. **(ITM-4.1)**

- **Information Technology Management Functional Area. Objective:** Ensure DoD vital information resources are secure and protected. **Goal:** Build information assurance architecture and supporting services. **(ITM-4.2)**

- **Information Technology Management Functional Area. Objective:** Ensure DoD vital information resources are secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. **(ITM-4.4)**

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the Department of Defense. This report provides coverage of the Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from January through September 2000 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data for this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized information assurance as a systemic weakness as stated in the FY 1999 DoD Annual Statement of Assurance. However, we determined that the lack of current NIPRNet security policy guidelines was a material management control weakness for the ASD(C^3I) (finding A). Recommendations A.1.-A.3., if implemented will correct the material management control weakness. A copy of the report will be provided to the senior official responsible for management controls in the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Appendix B. Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to information assurance issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed at http://www.dodig.osd.mil. The previous reports most relevant to the subject matter of this report are listed below.

General Accounting Office

General Accounting Office Report No. AIMD 99-107 (OSD Case No. 1835), "DoD Information Security-Serious Weaknesses Continue to Place Defense Operations at Risk," August 1999.

General Accounting Office Report No. HR 99-1, "High Risk Series – An Update," January 1999.

Office of the Inspector General, DoD

Inspector General, DoD, Report No. D-2000-124, "Information Assurance Challenges - A Summary of Audit Results Reported December 1, 1998, through March 31, 2000," May 15, 2000.

Inspector General, DoD, Report No. PO 97-049, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," September 25, 1997.

Army Audit Agency

Army Audit Agency Report No. AA 99-5, "Information Systems Security Program Phase II Follow-On Validation," October 15, 1998.

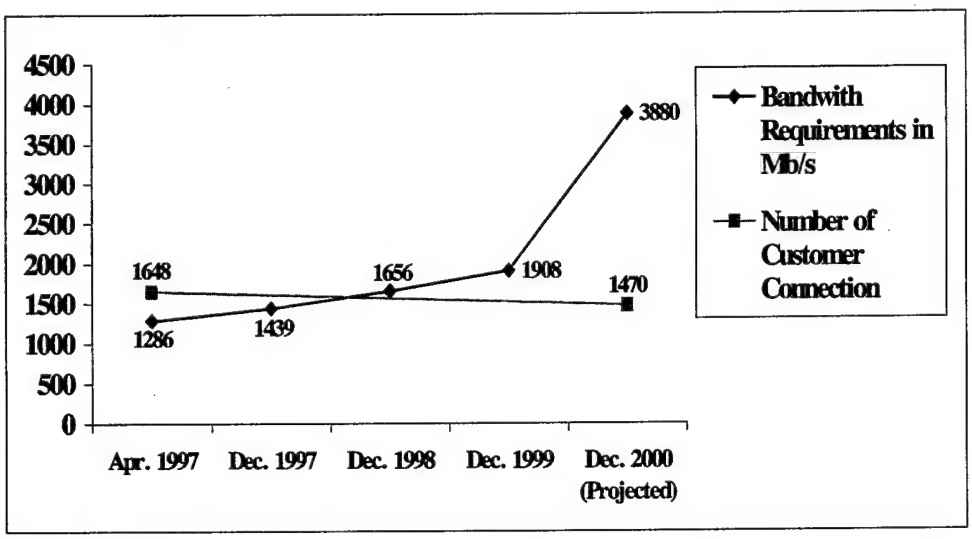
Army Audit Agency Report No. AA 97-214, "Information Systems Security Program," June 30, 1997 (FOUO).

Air Force Audit Agency

Air Force Audit Agency Project No. 96054027, "Data Communications Security," April 15, 1997.

Appendix C. NIPRNet Growth and Redesign Effort

NIPRNet Growth. NIPRNet users require more bandwidth every year, with the projected number of usage for the Year 2000 expected to double from the previous year. The increase in bandwidth is likely due to the increase in technology (video, audio, new applications) that is using the NIPRNet. As the number of customer connections decrease from year to year, the amount of bandwidth required per connection grows significantly. Figure 2 shows the actual and projected NIPRNet bandwidth requirements and customer connections.



Source: DISA

Figure 2. NIPRNet Global Customer and Bandwidth Trends

NIPRNet Redesign Effort. The goal of the NIPRNet redesign is to design the Continental United States portion of the network to handle both current and future traffic requirements. The redesign will result in increased performance, higher availability, additional security, and a reduced cost. To accomplish this goal, the NIPRNet will be segmented into six regions based roughly on geographic locations. Each region will have a dedicated Joint Interconnection Service connection to the Internet. The goal is to isolate each region's Internet traffic to that region's Joint Interconnection Service connection, which will ease traffic congestion on the NIPRNet backbone. Another goal of the regional network is to isolate local data traffic from the other NIPRNet regional segments.

The NIPRNet redesign consists of two phases. Phase one, completed in July 1999, involved upgrading routers and installing the six regional Joint Interconnection Service connections. Phase two consists of segmenting the NIPRNet into the six regional networks. The advantages of the NIPRNet redesign focus on four principal areas: performance, security, availability, and cost.

- Performance: Performance is improved by isolating local data traffic onto regional segments. Because of this, throughput (the capacity or amount of data that can be sent through a given circuit) and available bandwidth on the NIPRNet backbone is improved.

- Security: Newly installed routers will supplement NIPRNet security by adding in current network operating system security features.

- Availability: Newly installed routers and their associated power supplies will provide redundant capabilities.

- Cost: Cost per kilobit ratio is predicted to decrease by 55 percent once the redesign efforts are complete.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller/Chief Financial Officer)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
  Director, Program Analysis and Evaluation
Assistant Secretary of Defense (Command, Control Communications, and Intelligence)
  Deputy Assistant Secretary of Defense, Deputy Chief Information Officer
  Deputy Assistant Secretary of Defense, Security and Information Operations
    Director, Infrastructure and Information Assurance

Joint Staff

Director, Joint Staff

Department of the Army

Commander, U.S. Army Forces Command
  Deputy Chief of Staff, Command, Control, Communication and Computers
  Commander, Fort Irwin
Commander, Army Signal Command
  Director, Army Network and Systems Operation Center
Director of Information Systems for Command, Control, Communications and Computers
Chief Information Officer
Auditor General, Department of the Army

Department of the Navy

Chief Information Officer
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  Commander, Defense Information Systems Agency Area Command - Columbus
  Inspector General, Defense Information Systems Agency
Director, National Security Agency
  Inspector General, National Security Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

This page was left out of original document

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

December 1, 2000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

MEMORANDUM FOR DoD INSPECTOR GENERAL

SUBJECT: Audit Report on the Unclassified but Sensitive Internet Protocol Router Network Security Policy (Project No. D2000AS-0085)

This office has carefully reviewed and considered the Draft Audit Report, including findings and recommendations. The following comments are furnished.

Recommendation A1. The audit report background discusses PBD 417C, "Information Services, " and the Waiver Board directed therein. Building upon that concept, this office has expanded the scope of this process to enable the DoD CIO to better manage the Global Information Grid on an Enterprise basis, in compliance with the Clinger-Cohen Act of 1996 and Title 10, U.S.C., Section 2223.

1. The ASD (C3I) chairs the Waiver Board in his role as the DoD CIO.

2. Addition of three Board members adds depth to the process. To ensure Warfighter representation, we have added the Joint Staff/J6, as a voting member. To furnish technical advice, we have added the Director, DISA, as a non-voting member. Finally, to ensure an open forum with full disclosure, we have added the CIO of the DoD component requesting the waiver. These additions are important because the DoD CIO must govern the GIG, be familiar with the requirements, and insist that the WAN/MAN provider (DISA) continue to expand capabilities to meet emerging needs which often "push the envelope" of present capabilities.

3. The Waiver Board has instituted a Panel to administer the process. The Board first met on 3 Mar 00, and approved establishment of the GIG Network Waiver Review Panel. The Panel has been extremely active in the areas of legacy network migrations (to the DISN) and in adjudication of requests for waiver from use of the DISN to satisfy wide and metropolitan area (WAN/MAN) requirements. The Panel has also adjudicated a backlog of 121 NIPRNET CAP waiver issues. Since elimination of the backlog, waivers are generally adjudicated within two weeks of DSAWG review, and if granted the duration of the waiver is only (1) so long as it is deemed essential or (2) for one year, whichever is sooner. This technique is designed to force automatic annual review of any waived solution. The DISA NIPRNET staff tracks waived solutions. The Panel's latest initiative is to publish clear criteria to be used in the adjudication of NIPRNET CAP waiver requests.

4. In his role as Chairman of the GIG Network Waiver Review Panel, COL Neil Putz, (703) 607-0466, is required to brief each regular session of the CIO Executive Board. COL Putz routinely briefs the progress of the NIPRNET CAP certification effort, and as a result the DoD Component CIOs have sharpened their focus on attaining certification and on providing timely progress reports. Enclosure 1 depicts success over the past three months.

Final Report Reference

Recommendation A2. The report mentions the DepSecDef tasking to incorporate the GIG Network Policy into DoD issuance(s) by February 2001. The action officer for this important task is Mr. Tony Simon, (703) 607-0482. We see a requirement for two products, a DoD Directive and a DoD Instruction. The directive will capture the major precepts expressed in DoD CIO Guidance and Policy Memorandum No. 4-8460, "Department of Defense Global Information Grid Networks" (Enclosure 2) and Memorandum No. 10-8460, "Network Operations" (Enclosure 3). The directive will also incorporate the intent of the 22 Aug 99 ASD (C3I) memorandum, "Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)." In fact, the GIG Network Waiver Review Panel has been addressing this documentation concern since August 2000, and the issue was discussed as a part of the proceedings of Waiver Panel #13, held on 5 Sep 00 (Enclosure 4).

In September the DoD CIO tasked COL Putz to document the waiver process in a DoD Instruction. This instruction will formalize not only the legacy network migrations and the DISN mandate for WAN/MAN requirements, but will incorporate the interim guidance outlined in Recommendation A.1. The milestone for this issuance is February 2001, as previously mentioned.

Recommendation A3. As mentioned in our response to Recommendation A1, para 3, we have required a stringent tracking mechanism for all waivers. Our Waiver Panel Chairman has closely collaborated with the DISA waiver staff to define the requisite elements of the waiver database, and to emphasize the DoD CIO oversight of the waiver tracking process.

Our GIG Network Waiver Process website will soon be expanded to incorporate the NIPRNET CAP policies and procedures. If you have further questions regarding our efforts, my action officer is COL Neil Putz, 703-607-0466.

John L. Osterholz
Director
Architectures & Interoperability Directorate
OASD(C3I) DASD(Dep CIO)

Attachments a/s

Omitted because of length. Copies will be provided upon request.

Fort Irwin Comments

DEPARTMENT OF THE ARMY
HEADQUARTERS, NATIONAL TRAINING CENTER AND FORT IRWIN
FORT IRWIN, CA 92310-5000

REPLY TO ATTENTION OF
AFZJ-CG

MEMORANDUM FOR Department of Defense Inspector General, Office of the Assistant Inspector General for Auditing, Acquisition Management Directorate (Attn: Ms. Wanda A. Hopkins), 400 Army Navy Drive, Arlington, VA 22202

SUBJECT: Audit Report on the Unclassified but Sensitive Internet Protocol Router Network Security Policy (Project No. D2000AS-0085)

1. The following is submitted in response to the recommendations identified in the Audit Report on the Unclassified but Sensitive Internet Protocol Router Network Security Policy.

2. The DOD IG Audit recommended that the Commander, Fort Irwin:

a. Coordinate with the Defense Information Systems Agency (DISA) to identify and implement needed technical solutions to Fort Irwin's problems connecting to the Internet via the Unclassifed but Sensitive Internet Protocol Router Network. Fort Irwin's response: Concur. Fort Irwin has coordinated through FORSCOM, who in turn has coordinated with DISA, and has restructured the path and increased the bandwidth by which Fort Irwin reaches the Internet via the Unclassifed but Sensitive Internet Protocol Router Network.

b. Disconnect the commercial Internet connection until an Assistant Secretary of Defense (Command, Control, Communications and Intelligence) waiver is obtained or a technical solution is developed. Fort Irwin's response: Concur. Fort Irwin has disconnected the commercial Internet connection as of 29 September 2000, and has requested through FORSCOM that the request for waiver be withdrawn as of 10 October 2000.

3. Point of Contact for this information is Mr. Richard E. Schmalzbach, (760) 380-3002 or DSN 470-3002.

JAMES D. THURMAN
Brigadier General, U.S. Army
Commanding

U.S. Army Forces Command Comments

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY FORCES COMMAND
1777 HARDEE AVENUE SW
FORT MCPHERSON GEORGIA 30330-1062

AFDCG-IR (36-5) 4 DECEMBER 2000

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL, OFFICE OF THE ASSISTANT INSPECTOR GENERAL FOR AUDITING, ACQUISITION MANAGEMENT DIRECTORATE, 400 ARMY NAVY DRIVE, ARLINGTON, VA 22202

SUBJECT: DODIG Draft Report, Audit of Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) Security Policy

1. Reference subject DODIG draft report dated 25 September 2000.

2. Headquarters, U.S. Army Forces Command (FORSCOM) and Fort Irwin have reviewed the subject report and provide the following comments. Overall, Forces Command agrees that there was an absence of clear guidance that defined the roles in the internet waiver process, as discussed in finding A. However, Forces Command does not agree with the facts as presented in the report that Forces Command delayed actions to process the Fort Irwin waiver and inferences that Forces Command was not involved in review and processing of the request for waiver.

3. The following comments are being provided to address the facts and recommendations addressed in the finding. The comments are keyed to the specific report paragraphs and recommendations.

(a) Page 8 of the draft report concluded that Forces Command "delayed" the processing of the waiver request. We disagree with this conclusion. First, there was an absence of clear guidance from DOD that defined the roles in the internet waiver process. This was documented in finding A of this draft report. Second, the allegation that FORSCOM "delayed" the waiver process is incorrect. Forces Command was actively involved in the waiver process and has taken numerous actions to work with Fort Irwin and Defense Information Systems Agency (DISA). A list of actions that we have been involved in are shown at the enclosure. These actions were also discussed with the DODIG team during their visit to HQ, Forces Command on 28 August 2000.

(b) Page 8 of the report concludes that due to the connection with a commercial internet service provider (ISP), the ability of DISA to maintain control of the NIPRNET was impaired and the security posture of the NIPRNET put at greater risk. We disagree with this conclusion. The commercial ISP connection went through the Army Security Router, as does traffic over the regular NIPRNET connection. Further, Fort Hood submitted a waiver that was approved and their connection with a commercial ISP went through the Army Security Router. As such, it is our opinion that the risks at Fort Irwin were minimal.

Final Report Reference

AFDCG-IR
SUBJECT: DODIG Draft Report, Audit of Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) Security Policy

(c) Page 12, Recommendations.

B.1. "Coordinate with the Defense Information Systems Agency (DISA) to identify and implement needed technical solutions to Fort Irwin's problems connecting to the Internet via the Unclassified but Sensitive Internet Protocol Router Network."

Command Comments: Concur. Forts Irwin and Forces Command, in conjunction with DISA, identified the necessary technical solutions. The Fort Irwin NIPRNET connection was upgraded on 21 September 2000. All Fort Irwin users are now connected to the Internet via the NIPRNET.

B.2. "Disconnect the commercial Internet connection until an Assistant Secretary of the Defense (Command, Control, Communication and Intellegience) waiver is obtained or a technical solution is developed."

Command Comments: Concur. In conjunction with actions taken to recommendation B-1, the commercial Internet connection was disconnected on 29 September 2000. Fort Irwin has also initiated actions to withdraw the waiver request.

4. For additional information, please contact me at (404) 464-5404.

FOR THE COMMANDER:

Encl

DENNIS G. JOE
Chief, Internal Review
U.S. Army Forces Command

Omitted because of length. Copies will be provided upon request.

2

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Thomas F. Gimble
Mary Lu Ugone
Wanda A. Hopkins
Dianna J. Pearson
Richard B. Vasquez
Stuart W. Josephs
Cristina Maria H. Giusti
James S. Moon
Brian L. Zimmerman
Dan B. Convis
Peter C. Johnson

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Unclassified but Sensitive Internet Protocol Router Network Security Policy

B. DATE Report Downloaded From the Internet: 12/20/00

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 12/20/00**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.